

## DOOR ACCESS CONTROL AND KEY MANAGEMENT SYSTEM AND THE METHOD THEREOF

### Field of the Invention

- The invention relates generally to a security system and particularly to a
- 5 system and method for controlling physical access to doors and managing keys via a communication network.

### Background of the Invention

- Virtually all private residences, businesses and governments employ locks
- on all exterior doors and many interior doors to control physical access to premises
- 10 and vehicles, and to protect valuable contents and occupants from outsiders. The technology of locks and related security products have developed to provide a very wide range of choices in security levels, locking mechanisms, key types and other features. Available "key" technologies include, among others, various kinds of mechanical keys, magnetically coded swipe cards, so-called "smart" cards with
- 15 embedded microelectronic devices, plastic or metal cards coded with mechanical holes, short range radio frequency (RF) or infrared (IR) transmitters with coded signals, and various keypad arrangements requiring the user to input a pre-determined unlocking code.

- Presently, keys are generally associated with one or a few doors, and
- 20 therefore, access to the keys, i.e., the use of the doors, is controlled by the owner of the premises or vehicle to which the door allows access. The current system of lock usage leads to a number of problems both for the owners of premises and vehicles with lockable doors and for individual users. Most individual users are forced to carry and manage a large number of mechanical keys and/or cards. Also, it is an
- 25 issue to remember a number of passwords or keypad numbers and which key fits which lock, especially for keys which are used infrequently. Lost keys may result, in the case of mechanical keys, in a need to replace or re-key all locks with which the keys were associated. If a number of individual users have keys to a single door and one is lost, all key holders must be contacted and provided with new keys.

As well, passwords or keypad numbers can be inadvertently or deliberately revealed, thereby lessening security and usually resulting in a need to re-program the lock to accept a new code. Then, when code locks must be re-programmed, all authorized users must be informed of the new code and they must, therefore  
5 remember yet another code.

Also, keeping track of who has keys to which doors can be an issue and this becomes more complex, as in many business situations, the more doors and employees there are.

Further, if individuals are permitted to access some parts of a facility but not  
10 others, then a multiplicity of keys is required, adding to the problem of key management for both business and individual. And temporary access to premises by, for example, cleaning staff or neighbours, is difficult to control and monitor and, thus, reduces security.

Access to premises in emergency or potential emergency situations, such as  
15 by fire departments in the event of a fire alarm, usually requires forced entry, causing structural damage and consequent repair expenses.

Most businesses and many homes make use of monitored alarm systems in addition to door locks, requiring individual users both to carry keys for the premises and to remember alarm codes.

20 Access control systems exist that solve some of the problems by means of wired connections to the doors for which access is being controlled. Some of these systems can communicate between locations via wide area networks. Generally, such systems require special software and computer systems on or near the premises being protected. Often dedicated monitoring equipment and stations are  
25 required. These systems are costly to install and operate and are oriented towards larger organizations. These systems also do not extend to controlling access to locations where wired connections are impractical.

A number of other locking and access control systems have been devised. For example, it is known to employ wireless communication between a secure door

and remote site in order to obtain authorization. While these systems are successful in solving some of the problems mentioned above, they are usually too costly or require too much technical support to be of use to private residences or small businesses. In addition, none of the technologies employed thus far address the problems of the individual user who must deal with a large number of keys and/or codes.

Accordingly, there is a need to provide an improved system and method for physical access control, in which most of the above conventional problems and disadvantages can be solved.

## 10 Summary of The Invention

According to one aspect of the present invention, there is provided a door access control and key management system in which a number of doors and door users are involved. The system comprises (a) a communications network; (b) a door/key administering system for storing a key unique to each of the users, for storing an identification code unique to each of the doors, and for assigning access authorization to at least one user for each door, the door/key administering system being communicatively connected to the communications network; and (c) a door lock/control assembly mounted on each door for reading the key presented by the user, for verifying that the key has access authorization, and for operating the door in response to the authorization for access, the door lock/control assembly being communicatively connected to the door/key administering system via the communications network; (d) whereby a user can gain access to the doors authorized to the user with a unique key and each door can provide access to the user or users assigned thereto.

According to another aspect of the present invention, there is provided a method of controlling access to a plurality of doors by a plurality of door users via a communications network. The method comprises steps of: (a) storing a unique identification code for each of the doors in a server; (b) storing a unique key signature for each of the users in the server; (c) assigning to each door the unique keys having access authorization to the respective doors; (d) comparing a user's

key detected at the door to the keys having access authorization to the door in the server (e) authorizing access to the door; and (f) wherein the authorization step is carried out through the communications network between the door and the server and each user can gain access to the doors authorized to the user with a unique key and each door can provide access to the user or users assigned thereto.

According to another aspect of the present invention, there is provided a system architecture for controlling a plurality of door access control and key management systems. The system architecture comprises: (a) the plurality of door access control and key management systems noted above, the systems being communicatively and operatively connected to a communication network; and (b) a Meta server being adapted to serve as an address reference among the door access control and key management systems, the Meta server being communicatively and operatively connected to each of the door access control and key management systems via the communications network, wherein the Meta server contains the address of each door access control and key management system and its associated unique key ID codes and unique door ID codes and each door access control and key management system contains the address of the Meta server.

Other aspects and advantages of the invention, as well as the structure and operation of various embodiments of the invention, will become apparent to those ordinarily skilled in the art upon review of the following description of the invention in conjunction with the accompanying drawings.

#### Brief Description of the Drawings

Embodiments of the invention will be described with reference to the accompanying drawings, wherein:

FIGURE 1 illustrates a door access control and key management system according to one embodiment of the present invention;

FIGURE 2 illustrates the details of the door control/lock assembly of Figure 1; and

FIGURE 3 illustrates a system architecture according to another embodiment of the present invention for controlling a number of door access control and key management systems of Figure 1.

### Detailed Description of the Preferred Embodiments

In Fig. 1 there is shown a door access control and key management system according to the first embodiment of the present invention, which is generally denoted by reference numeral 10, and involves a plurality of doors and door users although a single door and user are illustrated for the convenience of description and understanding. Throughout the description and claims, the door includes all kinds of doors for access thereto to be controlled, including building entrance doors or interior doors, private house doors, vehicle doors, and safe doors, or all kinds of locks for other devices such as bicycles, padlocks. However, this invention is not limited to the doors and locks noted above.

Referring to Fig. 1, the system generally comprises a door control/lock assembly 20, a key administering system 40, a door administering system 60, and a communications network 80. The door control/lock assembly 20 is mounted on each door and communicatively connected to the key and door administering systems 40 and 60 via the communications network 80. In practice, the door administering system 60 and the key administering system 40 can be implemented as one single system equipped with the appropriate software program for carrying out both functions. In general, the door control/lock assembly 20 identifies a user 32 wanting to gain access to a door 30, and communicate with the key and door administering systems 40 and 60 to obtain authorization for access thereto.

In this embodiment, the communications network 80 includes an IP (Internet Protocol) communications network, which is accessible by the door control/lock assembly 20 via an HTTPS (Hyper Text Transport Protocol Secure) server. In such an Internet communication environment, the key administering system 40 and the door administering system 60 can be referred to as a key server system and a door server system as shown in Fig. 1. However, the communications network can employ any suitable network protocol.

All communication lines connecting the components of the system 10 employ encryption means for improved security.

The connection between the communications network 80 and the door lock/control assembly 20 can be accomplished via a wireless communication line. In such a case, an intermediate wireless transmitter/receiver 82 between them is provided as illustrated in Fig. 1. The means of wireless communication includes Bluetooth® or other short-range wireless communications circuitry, or a network access module consisting of Bluetooth® wireless communications circuitry, an Ethernet network interface and a battery backed up power supply. The network access module is located at a Ethernet port within the range of the Bluetooth® or other short-range wireless communications circuitry.

Alternatively, the means of wireless communication can include digital cellular wireless Internet access circuitry to provide greater range or for use where an Ethernet networks port is not convenient or available.

The system 10 further includes several other elements, which will be hereafter described.

Fig. 2 presents a detailed view of the door control/lock assembly 20 of the system 10. As illustrated in Figs. 1 and 2, the door control/lock assembly 20 mounted on each door 30 includes an electric door lock 22, an identification device 24, an embedded controller 28, a communicating means 26, and a battery for supplying power. The communicating means 26 establishes two-way communications with the communication network 80 via a wireless transmitter/receiver 82. The embedded controller 28 has appropriate software for controlling the door control/lock assembly 20 and any communications with other system components via the communications network 80. During operation, the door control/lock assembly 20 transmits via the communication network the identification data read by the identification device 24 to the key-door administering systems 40 and 60 and receives messages or signals from the administering systems as to whether the identified key is authorized. Details of the operation will be hereafter described.

The door lock 22 includes any lock that can operate in response to an authorization signal or message from the key and door administering system 40/60, or, in certain situations, from the embedded controller 28 of the door assembly 20.

The identification device 24 identifies the key wishing to gain access to the door. The identification device 24 can be a proximity card reader or swipe card reader or any other such device. Also, the identification device 24 can include a wireless receiver employing public key cryptography (PKI) technology or other secure communications technology to receive signals from a device carried by the user 32. In such a case, the key can be an electronic key such as a Dallas Semiconductor iButton®, a cell phone, a portable digital assistant (PDA) equipped with digital wireless capability, a personal communicator device, and an RF (Radio Frequency) tag device. For example, the tag device provides a short-range radio frequency signal that is coded to provide identification of the individual user. In addition, a biometric recognition device such as thumb-print reader or face-recognition device can be used as the identification device 24. A numeric or alpha-numeric key pad device can also be used. The key includes any device that can be sensed by the identification device used. For example, where the identification device is a numeric keypad, the key can be a numeric code.

As depicted in Fig. 2, the door control/lock assembly 20 can be equipped with more than one identification devices 24 and 24a to improve security or convenience. In such a case, for improved security, all keys are required in order for the system 10 to grant access. Also, for improved convenience, any one key can be required to gain access, therefore, the user 32 can carry one or more of a variety of key types, which correspond to the identification devices 24, 24a.

In the door lock/control assembly 20, the embedded controller 28 runs appropriate software for controlling the assembly 20 and carrying out an identification/authorization process by cooperating with the identification device 24 and communicating with the door and key server systems 40 and 60 via the communications network 80. Various identification/authorization software applications are well known in the art and any suitable one can be used. The embedded controller 28 comprises a local database or a memory 28a as shown in

Fig. 2. The local database or memory 28a stores, for example, data of the most recent and most frequent users of the door in encrypted form for security reasons. These data serve to speed up authorization process, or provides back-up capability in the event that the connection between the door assembly 20 and the administering systems 40 and 60 failed or is disrupted for any reason.

The embedded controller 28 in the door control/lock assembly 20 periodically conducts a self-test of its own functionality and records data from status sensors, which will be hereafter detailed.

Each door control/lock assembly 20 is provided with a unique identification code that is encoded in hardware and can be recognized by software programs running in the door control/lock assembly 20 and other software programs running in the system 10. The door administering system 60 serves to store the unique identification code for each of the doors and manage these ID codes. Also, each door is assigned an authorized user or users for access to the door from the door administering system 60. The door administering system 60 includes a database 62 where the unique ID code and the authorized users for each door are maintained and updated, when required, by a door administrator.

The door lock/control assembly 20 and the door server system 60 work together to provide a number of functions. For example, the door server system 60 records all uses of the door lock 22, including authorized entries and unauthorized attempts to enter. The door server system 60 also provides the necessary controls and communications capability to allow the door administrator to configure various security settings of the operation of the door control/lock assembly 20, in addition to the basic authorization settings of which keys are allowed to unlock which doors. These security settings include such functions as to who is authorized at specific times. Other additional functions include settings as to who is to be notified in the event of an alarm of low battery condition or a detection of hardware failure condition and how such notification is to take place (e.g., e-mail, pager, automated phone call, or the like.) Such factors as the amount of lead-time to report that low battery condition can also be set.

In this embodiment, the door administering system 60 periodically polls all connected door control/lock assemblies 20 to update frequent or most recent users saved in the embedded controller 28 and receive reports from the embedded controller self-test routines. If the embedded controller 28 in the door control/lock assembly 20 does not receive a poll from the door server system 60 within a pre-set interval, it can initiate a report to the server on its own.

A single door server system can provide these functions for a number of doors controlled by the same door administrator, or multiple door servers can be used. The same door server can also provide these functions for a number of different door administrators, but each door administrator is prevented from accessing the information pertaining to doors controlled by others. Any number of door server systems can run on the system at the same time. The information recorded in each door server database concerning the authorized entrances and exits through the door and the unauthorized attempted entrances and exits may be used in several ways. Reports can be generated when required.

The key administering system or server 40 serves to store a unique key for each of the users. The unique key is implemented by a key signature. The key signatures consist of the unique codes associated with each key, i.e., each user. The key signature serves to distinguish a key from any other keys. The type of these codes depends on the identification device 22 used on the door control/lock assembly 20. As examples, the key signatures can consist of coded numbers that have been magnetically written onto a normal magnet swipe card, if a swipe card reader is used as the identification device 24. The key signatures can be the unique hardware with embedded serial numbers assigned at manufacture to iButtons® if an iButton® reader is used as the identification device. The key signatures can be a signal unique to each user, if the identification device at the door is adapted to identify the unique signal from, for example, a Bluetooth® enabled cell phone or PDA (Portable Digital Assistant) carried by the user. The key signature can be a fingerprint recognition code if the identification device at the door is a fingerprint reader. The key signatures are stored in encrypted form in the key administering system 40.

The key administering server system 40 includes a database 42 that contains information on the keys and the doors to which each key is allowed access. The key server system 40 provides a number of functions by working together with the door control/lock assembly 20. In particular, the key server system records all use of the key, including authorized entries and attempts to enter using the key that were not authorized on a door-by-door basis.

The information recorded in the key server database 42 concerning the uses of the key to unlock various doors and any unauthorized attempted entrances and exits is used in various ways. Reports can be generated when required.

The key server system 40 can further provide the key administrator with reports of every instance of the use of the key that has been recorded anywhere on the system 10.

The key and door server databases 42 and 62 can be updated and viewed from a Web browser 52 connected to the communications network 80.

Since the door/key administering system 60/40 maintains logs of entries and exits, it is possible to access the database and determine whether anyone is in a secured area, and the identity of the person, if anyone is indeed in a particular area.

The system of Fig. 1 provides security means to control access by persons to building, rooms or vehicles, while gathering useful information. The system provides a means to allow a person access to some locations, while, at the same time, excluding access to other locations, this may be accomplished with only one access key per individual. Such access privileges can be variable according to time. The system provides a means to change the security settings such as access privileges of an individual quickly and easily from any location where an Internet connection and browser software are available. Information gathered by the system includes the time of all attempts to access the door and the identification of the individual attempting such access (if known) or the fact that an unknown individual attempted to gain access. Furthermore, the access privileges associated with the 'key' may be easily changed as circumstances change. This allows people potential

to have only one 'key' to open all of the doors in their lives while, at the same time, increasing security and convenience.

To deal with the occasional instance that the communications network 80 is not available and to speed up access for frequent users of a door, a local database 28a of frequent and most recent user authorized key signatures is stored in encrypted form in the door lock/control assembly 20 itself. Before sending a request message for authorization over the communications network 80 to the door server system 60, the embedded controller 28 in the door lock/control assembly 20 checks its own local database 28a and unlocks the door if a match is found between the signature of the key being presented and one that is stored in the local database 28a. The information that this action has taken place is then transmitted to the door server system 60 for storage subsequent to the door having been unlocked. Periodically the authorized keys in the local database 28a of the door assembly 20 are confirmed between the door assembly 20 and the door server system 60 by a series of encrypted messages over the communications network 80. This confirmation process can be initiated by the door lock/control assembly 20, or the door administering system or server 60. If a key signature that has been authorized is no longer authorized, then the key signature is removed from the local database 28a of the embedded controller of the door assembly 20.

Referring to Fig. 2, the door control/lock assembly 20 further includes other components to provide additional functions. Such a device can include a microphone and speaker assembly 23c and 25c. This serves to communicate with the door administering system or server 60 via the communications network 80, which then communicates with a designated door administrator 52 or other systems using e-mail, telephone or pager according to predetermined instructions stored in the door server system.

A doorbell/intercom signalling device can be provided and configured to send a message via email, pager or telephone to a designated monitoring administrator. The designated monitoring administrator can be located anywhere that an Internet connection and browser software are available.

As well, alarm devices such as motion detectors, smoke detectors, or water detectors etc. can be installed in the door lock/control assembly 20. The alarm device communicates with the door server system 60, which in turn communicates the alarm administrator according to instructions included in the database 62. Any other additional alarm components can be provided and configured to signal their condition in various ways and to monitor multiple locations that can be altered easily over time.

The door control/lock assembly 20 can further include a door open sensor 25a that detects whether the door is open or closed. A buzzer device 23a can also be included. If the door remains open for a period of time longer than a pre-set interval, then, the buzzer is sounded for a brief period before an alarm condition message is sent to the door administrator to deal with such alarms. If the door is closed after the sounding of the buzzer but before the sending of the alarm message, the alarm is not sent. Alternatively, the buzzer is not sounded and the alarm condition message is sent immediately. In either case, the information that the door open alarm condition was encountered is stored in the door server 60 as a reporting function. The pre-set interval for which the door may remain open before the buzzer sounds may be changed and may vary with time of day or it may be disabled for specific periods to accommodate various situations. Such changes or scheduling are accomplished by the door administrator accessing the door server system 60 via the browser 52.

Other system status sensors that may be part of the door control/lock assembly include a battery voltage sensor and a temperature sensor.

The door control/lock assembly 20 can also include a digital camera (still or video) that is configured to provide an image of the individual attempting to gain access to a person assigned to make human judgements on whether such individuals, not identified by the system should be allowed access. The judging person may then allow the individual in, if desired, by signalling the door control/lock assembly 20 from the Web browser 52. The camera may also be configured to record in the network databases, an image of all individuals attempting to gain access.

In Fig. 3, there is shown a system architecture according to the second embodiment of the invention, which is generally denoted by reference numeral 100, and can control a group of individual door access control and key management systems, for example, of the first embodiment of the invention, as shown Fig. 1.

5 The system architecture 100, in general, comprises a plurality of door access control and key management systems 110a and 110b, a Meta server 140, and a communications network 180. The communications network 180 includes an IP (Internet Protocol) communications network. For the convenience of description and understanding, two door access control and key management systems 110a and 110b are illustrated in Fig. 2, but a number of individual systems can be involved in  
10 to be controlled within a single system architecture.

Each door access control and key management system 110a or 110b involves a plurality of doors and door users, and includes a door lock/control assembly mounted on each door, a door/key administering system, and a  
15 communications network communicatively interconnecting the door lock/control assemblies and the administering system, as noted above in conjunction with the first embodiment of the invention of Fig. 1.

As depicted in Fig. 3, each door access control and key management system is communicatively connected to one another and the Meta server 140 via the  
20 communications network 180. The Meta server 140 is adapted to be aware of all instances of each door/key administering system and know how to contact them over the communications network 180. The Meta server 140 comprises a database 142, which contains unique ID numbers and the addresses of their associated administering systems. For example, the data base can contain a look-up table that  
25 associates each unique key ID code with the address of the corresponding key/door administering system, and also another look-up table that associates each unique door ID code with the address of the corresponding administering system.

Also, each door access control and key management system, i.e., each door/key administering system knows the location of the Meta server 140. The  
30 administering system contains the address of the Meta server 140.

The Meta server 140 is adapted to serve as an address reference, i.e., as a directory of addresses for those instances where the door/key administering system of one user needs to communicate with the door/key administering system of another user and the first system does not know the address of the second system.

5 Therefore, the first system can locate the second system through the Meta server via the communications network.

The Meta server can be accessed by an administrator responsible to maintain it, for example, through a Web browser 152 communicatively connected to the Meta server via the communications network 180, as shown in Fig. 3. Also, the database can be updated by the administrator when required.

10 Therefore, the door access control and key management system 110a communicates with other system 110b via the Meta server 140 such that the system 110a can provide access to its own doors for a user or users from other system 110b.

15 The Meta server 140 may be mirrored in a number of locations, in which case each Meta server is updated regularly so that all Meta servers can remain in the same state, for example, contain the same data.

When a door/key administering system has a new key ID number or door ID number added to it, the door/key administering system updates the information in the meta server database so that other door/key administering systems can communicate with the new key or door.

Other additional features and advantages according to the present invention are described below:

25 The door/key administering system has all of the unique ID codes of all of the doors and keys, and is aware of which door provides access for which key or keys. Thus, if a key ID code is required to be changed or deleted, its associated door/key administering system sends messages to all of the other door/key administering systems so that they can update their own relevant data. If a key is lost or stolen, its ID code is quickly and easily removed from all of the systems and then, the lost or

stolen 'key' may not be used by unauthorized persons. Attempts by someone to use the lost or stolen 'key' can be reported to, for example, the key server or the door server and such information may be useful in locating the missing key and the unauthorized key holder.

5 A special case exists for use in hotels, where the system of the invention allows the potential for hotel guests to avoid registering at the front desk. Instead, they can proceed directly to their rooms where 'registration' occurs as they are recognized at the hotel room door via their pre-arranged access identification or 'key'. The network databases can be connected to the hotel guest reservation and  
10 registration system.

Also, the system of the invention permits line-ups at hotel check ins or car rental agencies to be avoided while ensuring security for both the patron and the hotel or car rental agency. As well, keys not returned to hotels or car rental agencies are an expense and a potential security problem. The system removes  
15 both the expense and the security threat. Further, in a hotel with this system installed, hotel staffs have the means to know if someone is in a room without disturbing the occupant. The need for 'do not disturb' signs is eliminated and hotel guests will be disturbed much less frequently.

Fire Departments and other emergency crews can be allowed easy access to  
20 a building in emergency situations if door administrators authorize the use of a Fire department key. Emergency workers can also be allowed access to information on the door server which allows them to determine with much greater certainty whether anyone is actually in a burning building.

Many home owners with pets can configure a residential door to be operable  
25 by the pets themselves such to allow the pets access to and from the house while still providing security against access by other animals or by human intruders. A key can be assigned to allow the pet to use a pet door at will while keeping it locked to others. Times of operation can be set by the pet owner via a Web browser. Via the browser, as well, the pet owner can be informed as to whether the pet is in or out,  
30 how many times the pet has gone in/out etc. An example of such a key is an RF tag

device. These tags provide a short-range radio frequency signal that is coded such that the animal (and possibly its owner) can be identified by reference to a registry of such tags. The tag may either be implanted or mounted in a pet collar.

- 5 If a 'key' is lost or stolen it can be quickly and easily replaced for all its uses with no chance that the lost or stolen 'key' may be used by unauthorized persons. Attempts by someone to use the lost or stolen 'key' can be reported to the key server database owned by the rightful key owner and such information may be useful in locating the missing key and possibly in apprehending the thief.

- 10 When an employee is terminated or quits a position, keys, which are not returned to the employer, are an expense and a potential security threat. This system removes both the expense and threat.

No special user software is required. The required software systems run within the doors for which access is being controlled and on servers that may be run by third party service providers.

- 15 Information logs on use of the physical access control system is recorded remotely from the door over the communications network.

There is no physical limit to the number of individuals that can be granted access to any door on the system.

- 20 The system allows the possibility for individuals to have one key that can be used for multiple situations, including their residences, various work situations, vehicles or any other places to which they may need access on a regular or occasional basis. These access privileges can be altered or scheduled easily and quickly to apply to specific times or to adapt to changing circumstances. Such changing circumstances may include moving to a new house, acquiring vacation property, changing jobs, acquiring a new vehicle, renting a vehicle, renting a hotel room, temporarily accessing the house of a friend or neighbour, or losing a 'key'. In the case of a lost or stolen 'key' (where biometric identification systems are not being used) the old key can be cancelled for all of its uses and a new 'key' can be
- 25

authorized quickly and easily from any place where an Internet connection and browser software are available.

While the invention has been described according to what are presently considered to be the most practical and preferred embodiments, it must be understood that the invention is not limited to the disclosed embodiments. Those ordinarily skilled in the art will understand that various modifications and equivalent structures and functions may be made without departing from the spirit and scope of the invention as defined in the claims. Therefore, the invention as defined in the claims must be accorded the broadest possible interpretation so as to encompass all such modifications and equivalent structures and functions.